INNOVATIVE: Journal Of Social Science Research
Volume 4 Nomor 1 Tahun 2024 Page 4614-4627
E-ISSN 2807-4238 and P-ISSN 2807-4246
Website: https://j-innovative.org/index.php/Innovative

Analisa Manajemen Risiko Pada Aplikasi E-Smart Di BKPSDM Lombok Tengah Menggunakan ISO 31000

Sri Wahyuni Putri[1✉], Maulana Ashari[2], Mardi[3], Sofiansyah Fadli[4]
STMIK Lombok
Email: srwhyunip838@gmail.com[1✉]

Abstrak

Dalam mempermudah perekapan aktivitas sehari-hari di dinas BKPSDM (Badan Kepegawaian dan Pengembangan Sumber Daya Manusia) kabupaten Lombok Tengah maka diterapkan aplikasi E-Smart yang merupakan aplikasi berbasis *website* yang digunakan oleh seluruh ASN (Aparatur Sipil Negara) yang terdiri dari PNS (Pegawai Negeri Sipil). Dengan adanya aplikasi ini memungkinkan adanya ancaman dan serangan yang menimbulkan risiko, yang mana hal tersebut bisa mengganggu proses penggunaaan aplikasi. Oleh karena itu, artikel ini bertujuan untuk mengidentifikasi risiko-risiko pada apllikasi E-Smart yang berfokus pada Metode ISO 31000. ISO 31000 merupakan framework yang diterbitkan *International Organization for Standarization* yang berisi pedoman untuk menerapkan manajemen risiko. Berdasarkan penelitian ini Terdapat 4 kemungkinan resiko yang masuk ke dalam *Level of Risk* Tingkat *High* yaitu Penyalahgunaan Hak Akses/ Uses ID, Data dan Informasi tidak sesuai, Listrik Padam, Server Down. Berikutnya ada 30 kemungkinan resiko yang masuk ke dalam *Level of risk* tingkatan *medium* yaitu Debu dan Kotoran, Human Error, Maintenance tidak terjadwal, Pegawai baru yang belum mengerti betul alur kerja system, *Hacking*, *Vandalism* (merusak fasilitas seperti perangkat computer), Kurangnya SDM secara kualitas dan kuantitas, System Error, Petir, *Cybercrime*, *User interface* aplikasi yang sulit dipahami, Data *Corrupt*/ Rusak, Overheat pada perangkat computer, Network Gagal, Web service mati tiba-tiba, kegagalan system jaringan/jaringan terputus, *Overload* Database (kelebihan penyimpanan), Memory Full, Kegagalan back up data, kerusakan atau dissfungsi pada *hardware*, Serangan Virus, CCTV tidak berfungsi dengan baik, Genset tidak berfungsi dengan baik, *Backup Failure* (kegagalan percadangan), Gagal *update*, Pencurian perangkat, Kehilangan Data, Gempa Bumi, Kebakaran, Peretasan terhadap jaringan. Serta terdapat 1 kemungkinan resiko yang masuk ke dalam *Level of Risk* tingkatan *low* yaitu Banjir. Kemudian dilakukan Pencegahan Risiko (*Risk Prevention*) dengan tujuan untuk mengurangi resiko yang terjadi aktivitas pencegahan ini tetap dirasa menguntungkan karena dapat memberikan rasa aman. Dikarenakan bahwa tidak sepenuhnya menghilangkan resiko,

akan tetapi masih memungkinkan untuk mengurangi presentase terjadinya resiko.
Kata Kunci: *ASN, E-Smart, ISO 31000, Manajemen Risiko*

Abstract

To make it easier to record daily activities at the BKPSDM (Agency for Personnel and Human Resources Development) Central Lombok district, the E-Smart application has been implemented, which is a website-based application used by all ASN (State Civil Apparatus) consisting of PNS. This application allows for threats and attacks that pose risks, which can disrupt the process of using the application. Therefore, this article aims to identify the risks in E-Smart application that focuses on the ISO 31000 Method.ISO 31000 is a framework published by the International Organization for Standardization which contains guidelines for implementing risk management.Based on this research, there are 4 possible risks that fall into the High Level of Risk, namely Misuse of Access Rights/Uses ID, Inappropriate Data and Information, Power Outages, Server Down.Next, there are 30 possible risks that fall into the medium level of risk, namely dust and dirt, human error, unscheduled maintenance, new employees who do not really understand the system workflow, hacking, vandalism (damaging facilities such as computer equipment), lack of human resources as a whole. quality and quantity, System Error, Lightning, Cybercrime, Application user interface that is difficult to understand, Corrupt/Damaged Data, Overheat on computer devices, Network Failure, Web service suddenly shuts down, network system failure/network disconnection, Database Overload, Full Memory, Failure to back up data, damage or dysfunction to hardware, Virus Attack, CCTV not functioning properly, Generator not functioning properly, Backup Failure (backup failure), Failed to update, Device theft, Loss Data, Earthquakes, Fires, Hacking of networks. And there is 1 possible risk that falls into the low Level of Risk, namely flooding. Then Risk Prevention is carried out with the aim of reducing the risks that occur. This prevention activity is still considered profitable because it can provide a sense of security. Because it does not completely eliminate risk, it is still possible to reduce the percentage of risk occurring.
Keywords: *ASN, E-Smart, ISO 31000, Risk Management*

PENDAHULUAN

Aplikasi E-Smart merupakan salah satu aplikasi yang ada di Badan Kepegawaian dan Pengembangan Sumber Daya Manusia (BKPSDM) berbasis *Website* yang mempermudah perekapan aktivitas atau kegiatan yang dilakukan selama dikantor. Dengan adanya aplikasi web ini maka akan sangat mudah dan efisien, terlebih untuk perkembangan teknologi untuk zaman sekarang sudah berkembang sangat pesat, semua layanan yang dibutuhkan saat ini sudah tersedia secara online. Selain itu bisa mengetahui perbedaan tugas sesuai pola penilaian lingkup kinerja. Mulai dari kepala perangkat daerah, kepala unit organisasi, dan jabatan pelaksana dan fungsional. Selain itu pada aplikasi ini sangat mudah untuk mereview perilaku kerja sejawat dan atasan (Fadlia et al., 2022).

Standar ISO 31000 merupakan standar yang dibuat untuk memberikan prinsip dan panduan umum dalam penerapan manajemen risiko. Standar ini menyediakan prinsip, kerangka kerja, dan proses manajemen risiko. Prinsip manajemen risiko merupakan fondasi dari kerangka kerja dan proses manajemen risiko, sedangkan kerangka kerja manajemen risiko merupakan struktur pembangun proses manajemen risiko (Aisyah & Dahlia, 2022). Beberapa masalah yang menjadikan kemungkinan adanya ancaman dan serangan yang menimbulkan risiko sehingga mengganggu dalam proses penggunaan aplikasi. (Punusigon & Sitokdana, 2022) Oleh karena itu pentingnya manajemen risiko sebagai bentuk dari penanganan risiko terhadap ancaman yang bisa muncul kapan pun Manajemen risiko juga dapat meminimalisir risiko-risiko, risiko sebagai probabilitas yang dapat di ukur melalui pembentukan tingkat kepercayaan. Oleh sebab itu perlu dilihat sebagai pendekatan praktis, yang dimaksudkan ke dalam rencana strategis dengan mempertimbangkan kekhususan lingkungan instansi baik internal maupun eksternal dan tetap waspada dalam pemantauan(Henrique et al., 2020)(Pangestu & Wijaya, 2020)(Moleong & Tanaamah, 2022).

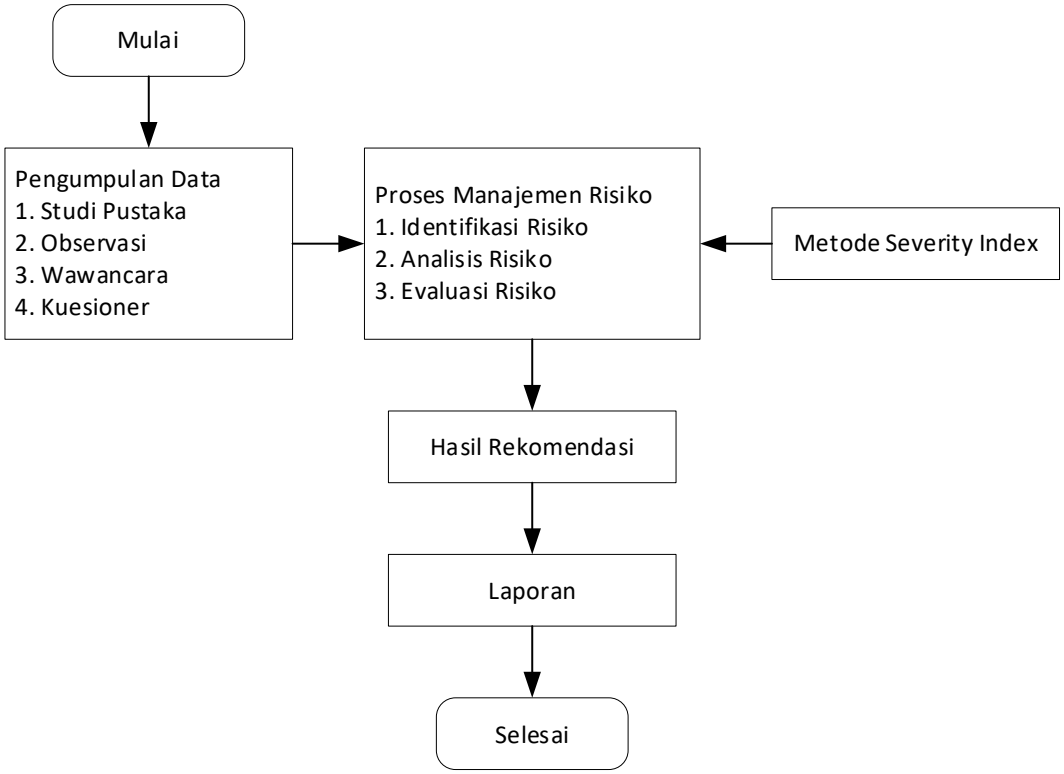
Adapun tujuan utama penelitian ini adalah untuk menerapkan manajemen risiko menggunakan standart ISO 31000 (Pamungkas et al., 2021), dalam rangka penanganan dan perlindungan terhadap aplikasi E-Smart yang digunakan oleh ASN (Aparatur Sipil Negara) di Kantor BKPSDM Kabupaten Lombok Tengah. Selanjutnya, penelitian ini bertujuan untuk menentukan tingkat risiko dari setiap risiko yang diidentifikasi, berdasarkan kriteria yang relevan dan mengacu pada standar ISO 31000(Mahardika et al., 2023).

Berdasarkan penjelasan yang peneliti paparkan diatas, peneliti melakukan kajian penelitian yang dilakukan oleh (Kanantyo & Papilaya, 2021) dengan judul Analisis Risiko Teknologi Informasi Menggunakan ISO 31000 (Learning Management System SMPN 6 Salatiga) yang terdapat 26 risiko yang menyebabkan aplikasi proses bisnis di SMP N 6 Salatiga menjadi terganggu. Dalam penelitian ditemukan 3 kemungkinan risiko dengan tingkatan High seperti Server Down, Web service yang sering mati, serta koneksi jaringan yang sering terputus. Kemudian terdapat 13 risiko dengan tingkatan medium, meliputi Kegagalan software, sistem crash, human error, koneksi jaringan tidak stabil, gempa bumi, petir, kerusakan hardware, proses maintenence tidak terjadwal, overload, serta data corrupt. Selain itu juga terdapat 10 risiko dengan tingkatan low, seperti penyalahgunaan hak akses, overheat, overcapacity, banjir, cybercrime, serangan virus, vandalisme, kegagalan backup, serta memori penuh. (Andika & Wijaya, 2022) terdapat 26 risiko yang menghambat kinerja dari proses bisnis yang berjalan di Pt. Trust Lerinvital Timur.

Berdasarkan penelitian ini, sudah ditemukan 3 risiko yang masuk dalam tingkatan high, seperti server down, webservice yang sering mati, dan juga koneksi jaringan yang sering terputus. Selain itu juga terdapat 13 risiko dengan klasifikasi medium, yang meliputi kegagalan software, sistem crash, human error, koneksi jaringan tidak stabil, gempa bumi, petir, kerusakan hardware, proses maintenence tidak terjadwal, overload, serta data corrupt. Dan juga terdapat 10 risiko dengan tingkatan low, seperti penyalahgunaan hak akses, overheat, overcapacity, banjir, cybercrime, serangan virus, vandalisme, kegagalan backup, serta memori penuh. Tujuan dan manfaat dari penelitian ini adalah membantu dalam menganalisis kemungkinan-kemungkinan risiko pada aplikasi E-Smart yang akan terjadi di kemudian hari, sehingga instansi dapat melakukan pencegahan sedini mungkin agar kemungkinan-kemungkinan resiko tersebut tidak terjadi dan mengganggu proses pekerjaan (Pangestu & Wijaya, 2020)(Harefa & Hartomo, 2022) (Lantang et al., n.d.). Sehingga perlu dilakukan Analisa risiko terhadap aset-aset dikarenakan risiko dapat muncul dimana saja dan kapan saja, jika tidak dianalisa sebelumnya maka tidak dapat dilakukan pengendalian terhadap risiko yang ada dan dapat menggangu kinerja. Serta dengan adanya dokumentasi risiko serta rekomendasi perlakukan risiko tersebut dapat menjadi acuan dalam memperlakukan risiko sebelum risiko-risiko tersebut menghambat kinerja instansi (Punusigon & Sitokdana, 2022).

METODE PENELITIAN

Teknik pengumpulan data yang digunakan yaitu metode wawancara, metode wawancara ini sarannya yaitu admin aplikasi E-Smart dengan tujuan mencari data berupa resiko yang timbul dari aplikasi tersebut. Metode yang digunakan adalah metode analisis manajemen resiko yang mengacu kepada ISO 31000 (Mahardika et al., 2023). Tahapan penelitian yang dilakukan dalam penyusunan penelitian ini dapat dilihat pada Gambar 1.



Gambar 1. Tahapan Penelitian

Pengumpulan Data

a. Studi pustaka, dilakukan dengan cara mencari buku yang relevan dengan penelitian serta mencari refrensi melalui jurnal nasional maupun internasional.
b. Observasi, dilakukan dengan cara mengamati suatu objek secara langsung dan dekat untuk memperoleh informasi yang tepat.
c. Metode wawancara, dilakukan wawancara langsung terhadap admin aplikasi E-Smart, dengan mengajukan pertanyaan kepada kepala bagian serta dari pihak pegawai mengenai risiko yang terjadi.
d. Kuisioner, penelitian dengan rangkaian pertanyaan menggunakan metode checklist yang bertujuan untuk mengumpulkan informasi yang terkait dari responden.

Tahap Identifikasi Risiko

Bertujuan untuk mengidentifikasi berbagai kemungkinan risiko yang muncul. Setelah diperoleh daftar risiko yang dapat terjadi maka mulai dianalisis faktor kemungkinan dan bagaimana dampak yang ditimbulkan dari risiko tersebut yang biasanya disebabkan oleh berbagai faktor internal maupun eksternal.

Analisis Risiko

Analisis risiko meninjau dua aspek risiko, yaitu *likelihood* dan *impact*. Analisis risiko juga dapat memberikan nilai pada risiko sehingga dapat ditimbang dan Tingkat risiko dapat

dikurangi. Data hasil dari proses identifikasi risiko kemudian dianalisa menggunakan metode Severity Indeks (Saputro, 2022) pada Langkah selanjutnya dengan metode manajemen risiko menggunakan kerangka kerja ISO 31000 sebagai kerangka acuan.

Evaluasi Risiko

Dengan tetap menggunakan acuan berupa matriks penilaian risiko, data dari tabel hasil analisis risiko berbagai tingkat risiko telah dikelompokkan menurut kode warna dan level Sangat Ringan, Ringan, Sedang, Berat, dan Sangat Berat. Risiko dikelompokkan berdasarkan level risiko yang dimulai dengan risiko tertinggi hingga risiko yang terendah.

Perlakuan Risiko/Hasil Rekomendasi

Terdapat beberapa risk treatment yang umumnya digunakan, yaitu; *risk prevention* (pencegahan risiko) dengan tujuan untuk mengurangi secara substansial kemungkinan terjadinya risiko, *risk mitigation* (mitigasi risiko) dengan tujuan untuk mengurangi dampak dari risiko, *risk sharing* (berbagi risiko) dengan tujuan untuk membagi risiko tidak hanya ke organisasi lain namun juga ke entitas bisnis ataupun individu, dan *risk retention* (retensi risiko) dikenal juga sebagai penyerapan, toleransi, atau penerimaan risiko.

HASIL DAN PEMBAHASAN

Kemungkinan resiko dari likelihood dan nilai impact pada proses sebelumnya akan disesuaikan dengan matriks resiko yang ada. Untuk melihat hasil dari penilaian resiko dari *Likelihood* dan *Impact*, dapat dilihat pada Matriks resiko berikut ini.

Tabel 1. Matriks Evaluasi Risiko

Likelihood	Sangat Sering	5	Medium	Medium	High	High	High
	Sering	4	Medium	Medium	Medium	High	High
	Sedang	3	Low	Medium	Medium	Medium	High
	Jarang	2	Low	Low	Medium	Medium	Medium
	Sangat Jarang	1	Low	Low	Low	Medium	Medium
	Impact		1	2	3	4	5
			Sangat Ringan	Ringan	Sedang	Berat	Sangat Berat

Pada tabel 2 merupakan hasil dari kemungkinan resiko-resiko yang sudah di masukan kedalam matriks evaluasi resiko sesuai dengan kriteria *Likelihood* dan *Impact* yang sudah di tentukan pada tahap sebelumnya.

Tabel 2. Matriks Evaluasi Risiko Berdasarkan nilai *Likelihood* dan *Impact*

Likelihood							
	Sangat Sering	5					
	Sering	4			R5,R6,R29	R7,R16,R17,R18	
	Sedang	3			R4,R10,R12,R19,R21 R22,R23,R24,R25 R26,R27,R28,R30 R31,R32,R33,R35	R9,R13,R14,R15,R20	
	Jarang	2		R1	R2,R3,R34	R8,R11	
	Sangat Jarang	1					
	Impact		1	2	3	4	5
			Sangat Ringan	Ringan	Sedang	Berat	Sangat Berat

Setelah kemungkinan-kemungkinan resiko dimasukan ke dalam matriks evaluasi berdasarkan Kemungkinan (*Likelihood)* dan Dampak (*Impact)* maka pada tabel 3 akan dijabarkan 35 kemungkinan resiko tersebut ke dalam level resiko dengan Tingkat *High*, *Medium* hingga *Low*.

Tabel 3. Level Resiko dari Kemungkinan Resiko

ID	Kemungkinan Resiko	*Likelihood*	*Impact*	*Risk Level*
R7	Penyalahgunaan Hak Akses/ Uses ID	4	4	High
R16	Data dan Informasi tidak sesuai	4	4	High
R17	Listrik Padam	4	4	High
R18	Server Down	4	4	High
R5	Debu dan Kotoran	4	3	Medium
R6	Human Error	4	3	Medium
R29	Maintenance tidak terjadwal	4	3	Medium
R9	Pegawai baru yang belum mengerti betul alur kerja system	3	4	Medium
R13	Hacking	3	4	Medium
R14	Vandalism (merusak fasilitas seperti perangkat komputer)	3	4	Medium
R15	Kurangnya SDM secara kualitas dan kuantitas	3	4	Medium
R20	System Error	3	4	Medium
R4	Petir	3	3	Medium
R10	Cybercrime	3	3	Medium
R12	User interface aplikasi yang sulit dipahami	3	3	Medium

R19	Data Corrupt/ Rusak	3	3	Medium
R21	Overheat (perangkat terlalu panas)pada Perangkat computer	3	3	Medium
R22	Network Gagal	3	3	Medium
R23	Web service mati tiba-tiba	3	3	Medium
R24	Kegagalan Sistem Jaringan/ Jaringan terputus	3	3	Medium
R25	Overload Database (kelebihan penyimpanan)	3	3	Medium
R26	Memory Full	3	3	Medium
R27	Kegagalan back up data	3	3	Medium
R28	Kerusakan atau dissfungsi pada hardware	3	3	Medium
R30	Serangan Virus	3	3	Medium
R31	CCTV tidak berfungsi dengan baik	3	3	Medium
R32	Genset tidak berfungsi dengan baik	3	3	Medium
R33	Backup Failure (kegagalan percadangan)	3	3	Medium
R35	Gagal update	3	3	Medium
R8	Pencurian perangkat	2	4	Medium
R11	Kehilangan Data	2	4	Medium
R2	Gempa Bumi	2	3	Medium
R3	Kebakaran	2	3	Medium
R34	Peretasan terhadap jaringan	2	3	Medium
R1	Banjir	2	2	Low

Pada tahap ini akan di berikan usulan-usulan yang dapat digunakan untuk memperlakukan kemungkinan-kemungkinan resiko tersebut. Dengan adanya usulan yang diberikan peneliti berharap resiko yang akan muncul dapat meminimalisir dengan baik agar aplikasi dapat berjalan dengan optimal dan tidak memiliki kerugian ketika resiko-resiko tersebut muncul.

Tabel 4. Usulan Perlakuan Resiko

ID	Kemungkinan Resiko	*Risk Level*	Perlakuan Resiko yang Diterapkan	Tindakan Usulan Resiko
R7	Penyalahgunaan Hak Akses/ Uses ID	High	Hak akses admin diberikan hanya kepada pengelola, dan jika terdapat permintaan dari pihak luar maka harus di awasi langsung oleh pengelola datacenter	(sudah ada aturan?) Mengadakan maintenance password secara berkala dalam 2 – 3 kali dalam setahun. Memberikan konfirmasi login yang berkaitan dengan pribadi user serta Memasang CCTV pada ruangan kerja kantor.

R16	Data dan Informasi tidak sesuai	High	Adanya backup data sebelumnya untuk dilakukan restore data jika terjadi kesalahan data dan informasi	Memastikan kembali data yang diterima sesuai dengan fakta yang ada dalam jangka waktu yang sudah ditentukan.
R17	Listrik Padam	High	Menggunakan backup listrik cadangan yaitu UPS	Memastikan UPS bisa digunakan dan melakukan pengecekan secara berkala
R18	Server Down	High	Adanya pengecekan secara berkala	Menentukan jadwal pengecekan berkala setiap 3 bulan sekali atau insidential
R5	Debu dan Kotoran	Medium	Ruang datacenter di bersihkan secara periodic	Melakukan pembersihan setiap hari disekitar dan pembersihan terhadap alat elektronik
R6	Human Error	Medium	Membatasi hak akses untuk masuk ke dalam datacenter	Selain membatasi perlu untuk memverifikasi hak akses
R29	Maintenance tidak terjadwal	Medium	Penjadwalan maintence secara berkala	Menentukan jadwal pengecekan berkala setiap 3 bulan sekali atau insidential
R9	Pegawai baru yang belum mengerti betul alur kerja system	Medium	Dilakukan pelatihan pada sistem versi development sebelum mengakses server production	Sosialiasi atau pelatihan kepada pegawai pasca development aplikasi
R13	Hacking	Medium	Menerapkan teknik - teknik pengamanan untuk mencegah proses hacking, seperti pergantian port access pada sistem, manajemen akun yang baik serta dilakukan pengecekan keamanan secara periodic	Menerapkan standar keamanan yang sudah diakui seperti ISO 27001/ ISO27003/ NIST CSF
R14	Vandalism (merusak fasilitas	Medium	Pembatasan hak akses ke data center,	Memantau CCTV setiap hari di gedung perusahaan. Dan selalu

	seperti perangkat komputer)		pengamanan rak server dengan kunci tunggal	mengecek setiap perangkat yang digunakan.
R15	Kurangnya SDM secara kualitas dan kuantitas	Medium	Tidak memberikan hak akses kepada pengguna sebelum mengerti sistem	melalukan penelitian dan bimbingan kepada pegawai
R20	System Error	Medium	Backup source code sistem secara berkala	Melakukan pengecekan pada framework sistem yang digunakan secara berkala
R4	Petir	Medium	Adanya penangkal petir pada gedung tempat datacenter	Hindari penggunaan lisrik setiap kali terjadi petir
R10	Cybercrime	Medium	Selalu dalam pengawasan	Pemantauan melalui CCTV pada ruangan yang penting dan selalu melakukan pengawasan
R12	User interface aplikasi yang sulit dipahami	Medium	Pengembangan user interface secara fleksibel sesuai feedback dari pengguna	Membuat tampilan pada user interface yang simple dan membuat petunjuk penggunaan aplikasinya
R19	Data Corrupt/ Rusak	Medium	Adanya backup data secara berkala	Melakukan backup secara berkala untuk mengantisipasi kemungkinan yang terjadi dan memproteksi PC dengan antivirus secara berkala untuk mencegah munculnya virus.
R21	Overheat (perangkat terlalu panas)pada Perangkat computer	Medium	Penjadwalan untuk monitoring suhu ruangan pada data center dilakukan	Mengontrol suhu ruangan agar selalu dingin dan selalu melakukan service AC (air conditioner) minimal sekali 6 bulan atau 1 kali dalam setahun
R22	Network Gagal	Medium	Tim jaringan khusus yang akan selalu standby	Sebagai upaya pencegahan terjadinya kegagalan jaringan perlu dijadwalkan maintenance secala berkala
R23	Web service mati tiba-tiba	Medium	restart webserver	Segera melakukan perbaikan saat web service mati dan memberikan informasi kepada pegawai lainnya.
R24	Kegagalan Sistem Jaringan/ Jaringan	Medium	Tim jaringan khusus yang akan selalu standby	Melapor ke bagian jaringan ketika koneksi jaringan terputus. Dan

	terputus			selalu melakukan pengecekan secara berkala
R25	Overload Database (kelebihan penyimpanan)	Medium	Monitoring kapasitas penyimpanan secara berkala dan menyediakan perangkat penyimpanan sebagai cadangan.	Melakukan refresh penggunaan db log, temp, dan RAM yang digunakan oleh aplikasi setiap seminggu sekali. Dan melakukan pengecekan db secara berkala
R26	Memory Full	Medium	Monitoring kapasitas penyimpanan secara berkala dan menyediakan perangkat penyimpanan sebagai cadangan	Selalu memonitoring penggunaan memori Bersihkan memori jika terdapat data yang tidak dibutuhkan dan melakukan pembesaran kapasitas memori
R27	Kegagalan back up data	Medium	Mengulangi backup data sampai berhasil di backup	Melakukan pengecekan secara berkala pada sistem dan database agar terhindar dari kegagalan back up data.
R28	Kerusakan atau dissfungsi pada hardware	Medium	Pengecekan hardware dilakukan secara berkala, jikalau tidak bisa diperbaiki maka diganti dengan yang baru	Pengecekan hardware setiap bulan atau setiap 3 bulan sekali, jikalau ada hardware yang rusak bisa di perbaiki oleh teknisi dan melakukan pencadangan hardware agar kalau ada hardware yang sudah tidak bisa di perbaiki bisa diganti dengan yang baru
R30	Serangan Virus	Medium	Membatasi hak akses agar tidak sembarangan mengakses ke server utama	Membatasi dan meverifikasi akses agar tidak sembarang orang dapat mengakses Database dan Server Utama
R31	CCTV tidak berfungsi dengan baik	Medium	Selalu melakukan pengecekan CCTV secara berkala	Melakukan pengecekan keamanan CCTV secara berkala minimal setiap hari atau bahkan 3 kali dalam seminggu
R32	Genset tidak berfungsi dengan baik	Medium	Pemasangan UPS untuk backup listrik.	Memastikan UPS bisa digunakan dan melakukan pengecekan secara berkala
R33	Backup Failure	Medium	Mengulangi backup data	Memperhatikan penggunaan

	(kegagalan percadangan)		sampai berhasil di backup	memori yang digunakan database agar jangan sampai penuh dan Membuat maintenance plan yang tepat. Melakukan backup data secara berkala.
R35	Gagal update	Medium	Melalukan *update* kembali dan mencari kesalahan dalam kegagalan agar dilakukan perbaikan	Setelah ditemukan beberapa kesalahan sistem segera melakukan perbaikan system agar tidak terjadinya kegagalan *Update.*
R8	Pencurian perangkat	Medium	Penjagaan 24 jam oleh security gedung dan penerapan hak akses yang baik	Pemantauan CCTV pada ruangan yang penting dan selalu melakukan pengawasan dan kalau bisa melakukan maintenance password agar tidak terjadi pencurian data.
R11	Kehilangan Data	Medium	Sudah ada backup data yang dilakukan secara berkala	Melakukan backup data dan Memeriksa beberapa bug yang ada dalam sistem.
R2	Gempa Bumi	Medium	Mengamankan perangkat percadangan di tempat yang cukup aman	Menyediakan server cadangan di tempat yang aman Atau menyediakan tempat yang cukup aman untuk perangkat yang menunjang SAP pada kantor tersebut.
R3	Kebakaran	Medium	Sistem penyiraman otomatis pada gedung jika terjadi kebakaran	Selalu dilakukan pengecekan terhadap alat penyiraman otomatis untuk menghindari alat tidak bisa berfungsi dengan baik
R34	Peretasan terhadap jaringan	Medium	Menerapkan teknik - teknik pengamanan untuk mencegah proses hacking, seperti pergantian port access pada sistem, manajemen akun yang baik serta dilakukan pengecekan keamanan secara	Menerapkan standar keamanan yang sudah diakui seperti ISO 27001/ ISO27003/ NIST CSF

			periodic	
R1	Banjir	Low	Ruang data center berada di lantai 3, untuk menjaga proses terjadinya kerusakan akibat banjir	Pengecekan berkala untuk memastikan bahwa datacenter berada di tempat yang aman

SIMPULAN

Penelitian manajemen resiko dengan menggunakan ISO 31000 yang telah dilakukan pada kantor BKPSDM (Badan Kepegawaian dan Pengembangan Sumber Daya Manusia) mendapatkan hasil yang mencakup penilaian resiko, identifikasi resiko, analisis resiko, evaluasi resiko hingga tahap perlakuan resiko. Dengan hasil akhir terdapat 35 kemungkinan resiko yang menghambat sesuai dengan tingkatan resikonya. Berdasarkan penelitian ini Terdapat 4 kemungkinan resiko yang masuk ke dalam *Level of Risk* Tingkat *High* yaitu Penyalahgunaan Hak Akses/ Uses ID, Data dan Informasi tidak sesuai, Listrik Padam, Server Down. Berikutnya ada 30 kemungkinan resiko yang masuk ke dalam *Level of risk* tingkatan *medium* yaitu Debu dan Kotoran, Human Error, Maintenance tidak terjadwal, Pegawai baru yang belum mengerti betul alur kerja system, *Hacking*, *Vandalism* (merusak fasilitas seperti perangkat computer), Kurangnya SDM secara kualitas dan kuantitas, System Error, Petir, *Cybercrime*, *User interface* aplikasi yang sulit dipahami, Data *Corrupt*/ Rusak, Overheat (perangkat terlalu panas) pada perangkat komputer, *Network* Gagal, *Web service* mati tiba-tiba, kegagalan system jaringan/jaringan terputus, *Overload* Database (kelebihan penyimpanan), Memory Full, Kegagalan back up data, kerusakan atau dissfungsi pada *hardware*, Serangan Virus, CCTV tidak berfungsi dengan baik, Genset tidak berfungsi dengan baik, *Backup Failure* (kegagalan percadangan), Gagal *update*, Pencurian perangkat, Kehilangan Data, Gempa Bumi, Kebakaran, Peretasan terhadap jaringan. Serta terdapat 1 kemungkinan resiko yang masuk ke dalam *Level of Risk* tingkatan *low* yaitu Banjir.

DAFTAR PUSTAKA

Aisyah, A. P., & Dahlia, L. (2022). *Enterprise Risk Management Berdasarkan ISO 31000 dalam Pengukuran Risiko Operasional pada Klinik Spesialis Esti*. *19*(02), 78–90.

Andika, D. Y., & Wijaya, A. F. (2022). *Manajemen Risiko Teknologi Informasi Menggunakan Framework Iso 31000:2018 Pada Pt. Trust Lerinvital Timur*. *5*(2), 111–118.

Fadlia, S., Putri, S. W., Tantoni, A., Ashari, M., & Fahmi, H. (2022). *Pelatihan Penggunaan Aplikasi E-SMART bagi Karyawan Sekretariat Daerah Bagian Organisasi*. *3*(1), 14–19.

Harefa, W., & Hartomo, K. D. (2022). Analisis Manajemen Risiko Dengan Menggunakan Framework ISO 31000:2018 Pada Sistem Informasi Gudang. *JATISI (Jurnal Teknik Informatika Dan Sistem Informasi)*, *9*(1), 407–420. https://doi.org/10.35957/jatisi.v9i1.1478

Henrique, G., Rampini, S., B, H. T., & A, F. T. B. (2020). *Faktor Keberhasilan Penting Manajemen Risiko dengan Munculnya ISO 31000 2018 - Analisis Deskriptif dan Isi Gabriel*. *39*(2019), 894–903. https://doi.org/10.1016/j.promfg.2020.01.400

Hutabarat, F. M., & Manuputty, A. D. (2020). Analisis Resiko Teknologi Informasi Aplikasi VCare PT Visionet Data Internasional Menggunakan ISO 31000. *Jurnal Bina Komputer*, *2*(1), 52–65. https://doi.org/10.33557/binakomputer.v2i1.792

Kanantyo, P., & Papilaya, F. S. (2021). *Analisis Risiko Teknologi Informasi Menggunakan ISO 31000 (Learning Management System SMPN 6 Salatiga)*. *8*(4).

Lantang, G. W., Cahyono, A. D., & Ngalumsine, N. (n.d.). *Analisis Risiko Teknologi Informasi Pada Aplikasi Sap Di Pt Serasi Autoraya Menggunakan Iso 31000*. 36–43.

Mahardika, F., H, M. A., Fatimah, S. A., & F, L. T. N. (2023). *Manajemen Risiko Teknologi Informasi Aplikasi E-Office ASN Menggunakan ISO 31000 : 2018*. *14*(02), 237–243. https://doi.org/10.35970/infotekmesin.v14i2.1877

Moleong, G. G., & Tanaamah, A. R. (2022). *Aplikasi Inlislite Di Dinas Kearsipan Dan Perpustakaan Provinsi Nusa Tenggara Timur*. *6*(2), 501–506.

Nieng, U. A. S., & Liperda, R. I. (2023). *Analisis Manajemen Resiko Aplikasi Mypertamina Dengan Menggunakan Iso 31000 Urbina*. *9* (2), 361–370.

Pamungkas, G., Bagas, M., & Atmojo, T. (2021). *Analisis Manajemen Risiko Teknologi Informasi Pada Website Umkm Xyz Berdasarkan Framework Iso 31000 Analysis Of Information Technology Risk Management On Umkm Xyz Website Based On Iso 31000 Framework*. *4*(1), 2–7.

Pangestu, R. P., & Wijaya, A. F. (2020). Analisis Manajemen Risiko Aplikasi SINTESA Pada Perpustakaan XYZ. *Jurnal Bina Komputer JBK*, *2* (2), 1–14.

Punusigon, F. G., & Sitokdana, M. N. N. (2022). Analisis Manajemen Resiko Aplikasi Simfoni Pada Dinas Ppa Di Kab. Minahasa Tenggara Menggunakan Iso 31000. *ZONAsi: Jurnal Sistem Informasi*, *4* (2), 25–36. https://doi.org/10.31849/zn.v4i2.10463

Rahmawati, A., & Wijaya, A. F. (2019). Analisis Risiko Teknologi Informasi Menggunakan ISO 31000 Pada Aplikasi ITOP. *Jurnal SITECH : Sistem Informasi Dan Teknologi*, *2* (1), 13–20. https://doi.org/10.24176/sitech.v2i1.3122

Saputro, C. D. (2022). *Analisis manajemen risiko proyek bangunan gedung bertingkat dengan metode severity index*. *6* (September), 140–147.